

REMARKS/ARGUMENTS

Claims 1-79 are pending. Claims 1-43 and 72 are amended.

Claims 1-79 are again rejected under 35 U.S.C. § 103(a) as being unpatentable over **Whitehouse** (US 6,005,945) in view of **Trieger** (US 6,065,117 [sic] **Trieger** is a U.S. Pat. No. 6,496,932). Applicant takes note that the current Office action (mailed on October 20, 2006) is the **ninth Office action** received from the Examiner, all of which cite **Whitehouse** as the primary reference. However, Applicant has repeatedly argued in detail that **Whitehouse** does not disclose a number of the limitations present in the independent claims. Applicant's attorney conducted two recent interviews with the Examiner on August 22, and 31, 2006, explaining in detail the differences between the **Whitehouse** and the claimed invention. Applicant respectfully request that each and every one of the arguments articulated below be sufficiently addressed by the Examiner.

Claim 1 includes, among other limitations, "a scalable server system communicating with the client system over a communication network," "wherein the server system is configured to process each security device transaction data record in a stateless manner," and "a stateless cryptographic module the users using one or more of the plurality of security device transaction data records stored in the database." Again, Applicants respectfully submit that the combination of **Whitehouse** and **White** does not teach, nor does it suggest the claimed invention.

First, regarding the claim limitation of "**wherein the scalable server system is configured to process each security device transaction data record in a stateless manner**," the specification defines "stateless" as "stateless, meaning the application does not remember the specific hardware device the last transaction utilized," and that "a PSD package can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package." (Page 8, lines 11-19). **Whitehouse** does not teach the above limitation because, the central computer 102 of **Whitehouse** stores the Customer Database 172 and the Transaction Database 174 in its **local memory** (RAM and NVM) 154. Also, the

transaction database 174 (local memory) stores **records** concerning each postage indicium generated by the secure central computer 102. (Col. 8, lines 30-34 and 54-61).

Therefore, "each transaction record" of Whitehouse (PSD or claimed "security device transaction data record") that is processed by each central computer 102 (assuming there are more than one central computer 102), contrary to the definition of "stateless," **must** remember the specific hardware (that is the specific central computer 102) that the last transaction utilized. This is because the data of that last transaction is stored in a specific hardware (local RAM of the specific central computer 102). Also, a postage transaction application in each central computer 102 has to rely on what occurred with the previous PSD package (transaction data record). That is, if Joe's previous transaction was performed on a first central computer and Joe's current transaction is being performed on a second central computer, the second computer needs to know what happened to Joe's previous transaction which is stored in the local memory 154 of the first computer, in order to be able to perform the current transaction correctly and completely. Otherwise, the transaction data will not be operated based on the most updated information stored in specific local memory 154 of a specific central computer 102.

As a result, a current transaction in the system of Whitehouse **must** remember the specific hardware device (first central computer 102) that the last transaction utilized and thus the second central computer 102 if there was one) can NOT process the transaction data in a stateless manner (because it **must** remember the specific hardware that the last transaction utilized, see above explanation), as required by the independent claim 1. Moreover, Trieger does not cure the above deficiencies of Whitehouse.

Second, regarding the claim limitation of "a stateless cryptographic module to authenticate the users using one or more of the plurality of security device transaction data records stored in the [remote from the users] database," the Office action admits that Whitehouse does not disclose the limitation. Nevertheless, the Examiner broadly points to Abstract, Summary of the Invention, FIG. 1, and col. 6 line 19 to col. 7, line 58 of Trieger as teaching the above limitation. However, Applicant fails to see any teaching or suggestion for the above limitation in the cited figure and text.

Trieger discloses a "stateless" client-server environment, in which the client/server "communication consists of transmissions bounded by disconnects and reconnects for each new request or response pair." (Col. 3, lines 13-16). The "stateless" terminology of Trieger is about communication links between the server and client. The invention of Trieger "replaces the information that tracks the results of the previous requests over established and reestablished communications links using an identifier string called a "key." Instead of an ever-increasing set of information transmitted from the client to the server and back, the embodiment described herein localizes the state between the client and server at the server and associates the state with the key string." (Col. 3, lines 40-46, underlining added.).

Additionally, "in this stateless Internet environment, the client 50 first establishes a logical or physical connection or link 54 with the server 52. It should be noted that the existence and/or permanency of any other connections or links between client 50 and server 52 (e.g. physical network cabling) does not affect the stateless nature of the logical connection or link 54. After establishing a connection (or link), the client 50 sends the request to the server 52 through the connection 54. After processing the request, the server 52 sends a response back to the client 50. The connection 54 is then broken or moved to an "inoperative" state by the server, the client, or both. This allows the server 52 to participate in the establishment of a new connection, receive a request, and transmit a response to another client." (Cited col. 6, lines 47-61, underlining added.).

Trieger stresses the context and definition of what he calls a "stateless environment" as "the server is typically in this initial state regardless of how many connections have been or will be established. This is the "stateless" nature of the client-server environment. As a result, the client 50 must communicate to the server 52 information resulting from or pertaining to previous communications in order to establish the previous "state" of communications, if client 50 wishes his new request to be processed relative to such communications. In the prior art, this is done by resending all the previous state information to the server 52 with the new request."

Trieger's invention tries to solve this problem by having "the client 50 instead send[ing] an identifier or "key," which the server 52 uses to identify any previously stored information for

various clients. The interaction between client 50 and server 52 in the preferred embodiment is described in FIGS. 3 and 4. The creation and validation of keys at the server 52 are described in FIG. 4." (Col. 7, lines 61-67, underlining added.). The descriptions of FIGs. 3 and 4 further explain the communication between the server And the client using the "key."

In summary, the system of Trieger is about a "stateless" client-server environment, in which the client/server communication consists of an identifier or "key." There is no teaching or suggestion in Trieger, alone or in combination with Whitehouse, about "a stateless cryptographic module to authenticate the users using one or more of the plurality of security device transaction data records stored in the [remote from the users] database."

Third, regarding the claim limitation of "**a scalable server system communicating with the client system**," the specification defines "**scalable**" as "An increase in the number of servers within the server system 102 will not negatively impact the performance of the system, since the system design allows for scalability. The Server system 102 is designed in such a way that all of the business transactions are processed in the servers and not in the database. By locating the transaction processing in the servers, increases in the number of transactions can be easily handled by adding additional servers [that is scalability]." (Page 8, lines 2-10, emphasis added.).

In the Office action, the Examiner (once again) points to the "one or more **postal service computers 180**" of Whitehouse as the scalable server system. Again, in the above-mentioned interviews, the Examiner pointed out that he really meant the central computer 102 of Whitehouse and not the postal service computers 180. Accordingly, the Applicant hereby submits arguments that none of the central computers 102 or postal service computers 180 of Whitehouse suggest the above limitation.

The postal service computers 180 communicate only with the central computer 102 and thus are NOT communicating with the client system. Also, the postal service computers 180 do NOT include a database remote from the users including information about the users; a stateless cryptographic module for authenticating the one or more users; and a plurality of security device transaction data stored in the database, as required by claim 1.

Similarly, the central computers of Whitehouse (that is a specific central computer 102) are NOT and can NOT be scalable. That is, one can NOT easily add additional central computers 102 in the system of Whitehouse, because the entire internal memory structure (hardware) of each central computer 102 needs to be modified. **This is because each central computer 102 of Whitehouse stores the Customer Database 172 and the Transaction Database 174 in its own local memory (RAM) 154** and the transaction database 174 (local memory) stores records concerning each postage indicium generated by the secure central computer 102. Therefore, if one adds an additional central computer in the system, the new central computer must be able to access the local memories (RAMs) of all other existing central computers in order to stay up-to-date for all the transactions that the system performs. One skilled in the art of computer architecture would readily realize that this is NOT an easy task and requires extensive re-design of the system architecture. Therefore, the central computers of Whitehouse having stored the transaction data in their local memories 154, are **not scalable**.

Fourth, Applicant still fails to see any **motivation to combine** Trieger with Whitehouse. The Examiner states that it would have been obvious to one skilled in the art to modify Whitehouse's system to include Trieger's stateless cryptographic modules "because this would have enhance [sic] the security of the system." Applicant respectfully disagree.

First, as explained above, there is no stateless cryptographic modules in Trieger. Second, it is not possible, without major architectural changes and a major overhaul of the system, as described above with respect to "first argument," to make the Whitehouse system a "stateless environment," as described by Trieger. Third, even if one could make the Whitehouse system a "stateless environment," the "stateless" client-server environment does not enhance the security of the already secured (by cryptography) system of Whitehouse. In fact, by making the Whitehouse environment a "stateless environment" as defined by Trieger, the system of Whitehouse becomes less secure, because multiple copies of the cryptographic keys need to be generated and stored in the local memories of the Whitehouse's computers. Fourth, Whitehouse is about postage dispensing and Trieger is about a session tracking method, therefore, they are from two different fields and cannot be combined. Fifth, each of the Whitehouse and Trieger

Appln No. 09/690,243
Amdt date November 17, 2006
Reply to Office action of October 20, 2006

references are **individually complete** and **functional in itself**, one skilled in the art of computer authentication would see no reason to add parts to any of them. For example, one skilled in the art of computer authentication would readily appreciate that adding the "stateless environment" of Trieger will not enhance the authentication of Whitehouse system, because Whitehouse system is already using encryption to protect its data.

In short, based on at least the above-mentioned **four arguments**, each of which deemed sufficient by itself, the independent claim 1 is patentable over cited references.

Independent claim 39 includes, among other limitations, "ensuring authenticity of the one or more users utilizing a respective security device transaction data record," "processing in a stateless manner each security device transaction data record in the server system," and "authenticating by a scalable cryptographic module the one or more users utilizing one or more of the plurality of security device transaction data record stored in the database." As discussed above, the combination of Whitehouse and Trieger does not teach or suggest the above limitations. Consequently, claim 39 is also patentable over cited references.


In short, independent claims 1 and 39 are patentable in view of the cited references. Dependent claims 2-38 and 40-79 depend from claims 1 and 39, respectively and include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested.

Appln No. 09/690,243
Amdt date November 17, 2006
Reply to Office action of October 20, 2006

If the Examiner believes that a telephone conference would be useful in moving this application forward to allowance, the Examiner is encouraged to contact the undersigned at (626) 795-9900.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By 
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS710969.1 - 11/17/06 3:32 PM